Hindawi
Mathematical Problems in Engineering
Volume 2018, Article ID 8025093, 12 pages
https://doi.org/10.1155/2018/8025093

Research Article

"Dose-Response" Vulnerability Assessment of Urban Power Supply Network: Foundation for Its Sustainability and Resilience

Haizhou Tang,[1] Xudong Zhao ,[1] Zhilong Chen,[1] Jiheng Xu,[2] and Xiaochao Su[1]

[1]*State Key Laboratory of Explosion & Impact and Disaster Prevention & Mitigation, Army Engineering University of PLA, Nanjing 210007, China*
[2]*Teaching and Research Center of Civil Air Defence, Army Engineering University of PLA, Nanjing 210007, China*

Correspondence should be addressed to Xudong Zhao; wxlmss@163.com

Received 8 August 2018; Accepted 4 December 2018; Published 20 December 2018

Academic Editor: Maria C. Cunha

Urban power supply network plays a vital role in maintaining the city operation. The vulnerability of power supply network in the face of events has been one of significant concerns. This study presents a new methodology and framework for "dose-response" vulnerability assessment of urban power supply network. This framework can explore the vulnerability of power supply network under two types of events: random type and intentional type. It also integrates a new metric that calculates the vulnerability of power supply network in both structural dimension and functional dimension. Taking the power supply network of a city in east China as an example, network vulnerability under different types of events was assessed, and the "dose-response" interrelationships between network performance and event scale under different types of events were thoroughly discussed. The results demonstrated that power supply network was more vulnerable to intentional events in both dimensions. For intentional events, power supply network was more vulnerable to degree-based attack than to betweenness-based attack. After that, the redundancy coefficient α of power supply network was optimized. The conclusion and some suggestions for future research were given in the end.

1. Introduction

The sustainable development of modern city mainly depends on the conservation of urban critical infrastructure networks, such as urban water supply network, power supply network, gas supply network, communication network, and transportation network, which are threatened by the increasing of natural and manmade disasters.

Urban critical infrastructure networks are the lifeline of the modern city and play a vital role in maintaining the operation of the city and residents' lives. Urban power supply network is one of the most critical infrastructure networks that provides energy for other networks. Therefore, the sustainable and resilient development of power supply network in the face of various natural and man-made events has been one of the concerns in engineering [1–3].

For the sustainable and resilient development of urban power supply network, the committed step is to assess the impact associated with the various domains of events [4]. Vulnerability assessment is a reasonable way to thoroughly observe the impact on entire infrastructure network caused by different domains and intensities of events [5–7]. According to available studies, vulnerability assessment is an essential step which quantitatively provides impact and consequence of infrastructure network for resilience and risk assessment [5, 8, 9]. For sustainability assessment of critical infrastructure network which is just beginning, the idea of combining resilience and incorporating risk was proposed and became popular [4]. Therefore, vulnerability assessment that scrutinizes the impact on power supply network associated with various domains of events should also be fundamental for the research of sustainability and resilience.

Different from available vulnerability study of infrastructure network, as the foundation of further research of resilience and sustainability, the vulnerability assessment of power supply network should have some new attributes.

(1) The domain extension of events: available vulnerability studies of infrastructure network mainly focused on the specific natural hazards such as earthquake, flood, and meteorological disasters, which randomly damage the components of infrastructure network components without subjective intent and selection strategy. However, the vulnerability of infrastructure network under malicious attacks was rarely considered in available research. With the increasing threats posed by global terrorism, urban power supply network will encounter the joint risks of natural disasters and malicious attacks. Therefore, for the vulnerability assessment of urban power supply network, the domain of events should expand from natural events to intentional attack.

(2) The dimension extension of impact: available vulnerability studies of infrastructure network usually concentrated on single structural dimension using a topological index to measure the structural impact of an infrastructure network [10–15]. But for sustainable development of infrastructure network, the impact of infrastructure on function, society, economic, or ecology should also be taken into consideration. In fact, many available studies also claim that the vulnerability and resilience assessment of infrastructure network should integrate four interrelated dimensions (technical, organizational, social, and economic) [16–18].

In order to address these two new attributes, it is necessary to establish an appropriate method to conduct the vulnerability assessment for power supply network. In general, "vulnerability" should be clear with respect to the impact of the infrastructure system due to the given event taken into consideration [9, 14, 19].

Haimes elaborated on the definition of "vulnerability" and its quantitative assessment and indicated that, to assess the vulnerability of an infrastructure system, the "dose-response" relationship between system performance and different scale should be thoroughly analyzed [5, 8]. Figure 1 shows two typical "dose-response" curves of system performance. In Figure 1, dash line A refers to the pre-event normal performance of system. B and C are two typical "dose-response" curves of system performance. With the increasing of dosage (i.e., event scale, which can be represented by the percentage of failed components), curve C shows a sustained decline trend of performance, while curve B shows an obvious rebound phenomenon of performance due to the internal adaption of system. Using this "dose-response" curve of system performance in different dimensions, we proposed a new method and framework to thoroughly assess and analyze the vulnerability of power supply network under different types of events.

According to the study of Haimes, we establish a "dose-response" vulnerability assessment framework which integrates a new method to assess the vulnerability of power supply network in both structural dimension and functional dimension. Using this framework we can fully address both new attributes needed by the vulnerability assessment of power supply network for the following reasons.

(1) This framework can thoroughly explore the impact of power supply network from the domain of natural events to intentional attack. In essence, different from intentional attack, natural events have randomness in terms of the failure of infrastructure network components and do not have subjective intent and a selection strategy. Therefore, all events can be divided into two basic types: random type and intentional type.

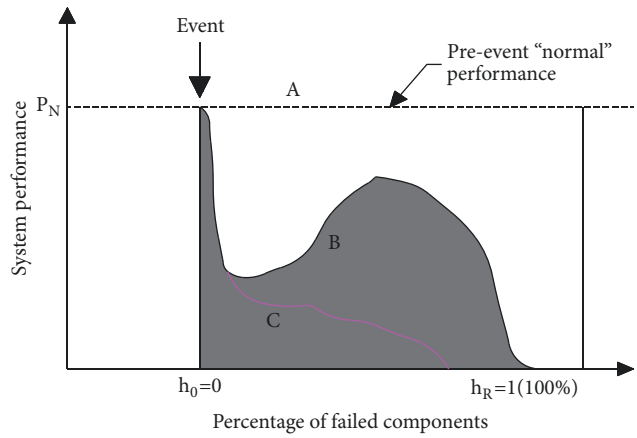

Figure 1: Typical "dose-response" curves of system performance.

(2) "Dose-response" vulnerability assessment can be conducted on multiple dimensions including structure, function, society, economy, and ecology. In the structural dimension, vulnerability assessment usually uses physical network index such as network betweenness index [7, 20], link density, and average node degree [10] to measure the impact of events on the network structure. In other dimensions, the emphasis is on measuring the impact of events on infrastructure function, society, economy, and ecology. It should be noted that the impact of events on society, economy, and ecology is usually caused primarily by the disturbance of infrastructure structure and function. Therefore, as the foundation for further research of sustainability and resilience, we first and foremost focus on the structural and functional dimension in the "dose-response" vulnerability assessment, and it is convenient to expand to other dimensions such as society, economy, and ecology in the future.

To illustrate the framework, we take the power supply network of a city in east China as an example to conduct vulnerability assessment. Through this case study, we thoroughly investigated the "dose-response" interrelationships between the structural performance, functional performance, and event scale under both random and intentional events. Then we calculated and compared the vulnerability of power supply network in structural and functional dimension. These interrelationships and conclusions can be foundational information for further research of sustainability and resilience.

2. Methodology for "Dose-Response" Vulnerability Assessment

2.1. Overall Framework. For the "dose-response" vulnerability assessment of power supply network, we need to build a response process of network performance that varies with different scale and types of events. Thus, "dose-response"

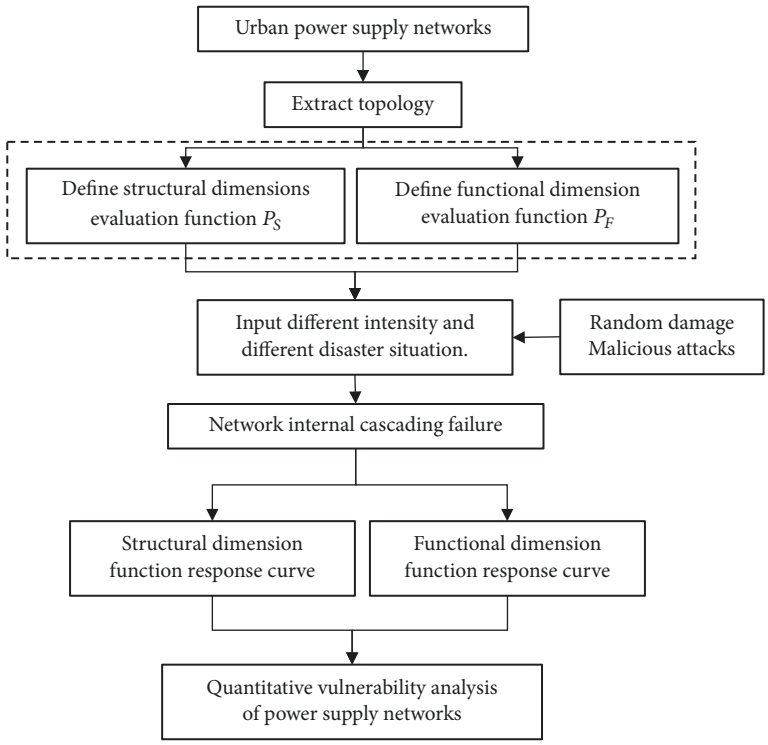

Figure 2: Framework for "dose-response" vulnerability assessment of urban power supply network.

vulnerability assessment provides a theoretical basis for resilience enhancing planning and sustainable development for infrastructure network.

Focusing on the urban power supply network, Figure 2 shows the overall framework for "dose-response" vulnerability assessment. To more exactly depict the "dose-response" curve of network performance in both structural and functional dimension, the cascading failure mechanism between the internal network components caused by initial event is introduced in the framework.

In order to elaborate on the framework shown in Figure 2, we divide it into six steps, and each step is explained as follows.

Step 1 (network preparation). Extract the network graph of the urban power supply infrastructure. Without the loss of operation characteristics of the power network, the network is simplified to the network graph model of nodes and edges using proper abstraction and simplification.

Step 2 (determine the performance function of the power supply network). We primarily focus on the performance in both structural and functional dimension as a foundation for the further vulnerability assessment in other dimensions.

Step 3 (input different event scale and types). Concerning the infrastructure network itself, we use the percentage of failed nodes directly caused by the event to represent the event scale. In this framework, we consider two event types: random type and intentional type. Random type refers to the random failure of power network nodes, which can reflect indiscriminate impact on the network components caused by natural disasters or other normal events. Intentional events refer to events such as terrorist attacks, which are based on people's subjective choice. The more important the nodes in the network are, the more likely they are to be attacked. For the power supply network, node importance can be measured using two indicators: node degree and node betweenness [21]. Thus, intentional type of events can further be divided into two types: degree-based attack and betweenness-based attack.

Step 4 (cascading failure process simulation). After the initial failure of network components directly caused by the event, the internal cascading failure will appear in the power supply network, which results in a larger scale impact on the structure and function of infrastructure network. In order to comprehensively and accurately assess the impact of events on the power supply network, we analyzed the cascading failure mechanism and introduced it into the framework.

Step 5 (obtain the "dose-response" curve of network performance with different event scale and types). For a given event (i.e., given scale and type), it is not difficult to obtain the initial performance change of infrastructure network directly caused by the event. Then, after the simulation of internal cascading failure, we can get the performance value of power supply network in each dimension. Therefore we can draw the "dose-response" curve to show the variation of network performance with the event scale in different dimensions.

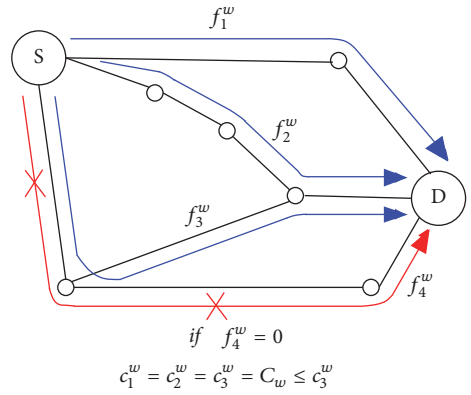

Figure 3: Wardrop's first equilibrium principle of network flow.

Step 6 (vulnerability calculation and suggestion providing). According to the "dose-response" response curve obtained in Step 5, we are able to calculate the vulnerability of network in structural and functional dimension, analyze the structural and functional weakness, and provide optimizing suggestions for the development of power supply network.

2.2. Performance Function in Different Dimensions. In this framework, we primarily focus on the "dose-response" vulnerability in both structural and functional dimensions as a foundation for the further vulnerability assessment in other dimensions. Therefore, in this section, suitable performance function for the structural and functional dimension was put forward, respectively, to measure the system state of urban power supply network.

2.2.1. Structural Dimension. In structural dimension, some structural indexes such as connectivity, average-betweenness, link density, and average node degree are often used to measure the structural performance of infrastructure network [10–14, 18, 20, 21]. In this study, we used generic minimal path cost and defined a metric to measure the structural performance of power supply network:

$$P_S = \frac{1}{n_W} \sum_{\omega \in W} \frac{1}{C_\omega} \tag{1}$$

where ω denotes a node pair through which power services are transmitted, W is the set of all node pairs, n_W is the number of all the node pairs, and C_ω denotes generic minimal path cost of each node pair in the network. This metric is derived from the N-Q method presented by Nagurney and Qiang and developed on the basis of network equilibrium theory [22]. It can be applied to evaluate the structural performance of infrastructure networks.

According to network equilibrium theory, the generic minimal path cost C_ω must follow Wardrop's first equilibrium principle (Figure 3) [22], which can be described as

$$\begin{aligned} c_k^\omega &= C_\omega \quad if \ \ f_k^\omega > 0 \ \forall k \in K^\omega, \ \omega \in W \\ c_k^\omega &\ge C_\omega \quad if \ \ f_k^\omega = 0 \ \forall k \in K^\omega, \ \omega \in W \end{aligned} \tag{2}$$

where k denotes a path that connects two nodes in pair ω, while K^ω is the set of all possible paths in the node pair ω, the service flow on path k is denoted by f_k^ω, and c_k^ω is the path cost on path k.

In this study, structural performance is described by C_ω, which is defined as the number of intervals between the two nodes in node pair ω. It can be seen that the definition of C_ω meets the requirement of (2) and Figure 3, and this definition is closely related to the physical topology status of power supply network. The higher the efficiency of ω to transmit services, the lower the C_ω value. When the connection between the two nodes is broken, C_ω tends to be infinity ($+\infty$) and $1/C_\omega$ approaches zero. When this occurs, services cannot be transmitted in node pair ω.

2.2.2. Functional Dimension. For the urban power supply network, functional performance should show the ability of network to provide power service. Likewise, there are also many available indexes that can be adopted to measure the functional performance. In the case study, functional performance P_F is characterized by the proportion of still running nodes under given event [23, 24], that is, after the failed nodes are removed, the proportion of nodes that are still in normal operational state and connected to the source node:

$$P_F = 1 - \frac{N_{\text{source, fail}}}{N_{\text{source, orig}}} \tag{3}$$

where $N_{\text{source,fail}}$ denotes the number of failed nodes (i.e., nodes in abnormal state or disconnected to the source node) after the impact of given event and $N_{\text{source,orig}}$ denotes the total number of nodes in the initial state.

To calculate the number of failed nodes $N_{\text{source,fail}}$, we should calculate the nodes directly impacted by the given event and the nodes overwhelmed by the subsequent cascading effect. For the given event scale and type, we firstly proportionally remove the nodes (including their adjacent edges) in a particular way. Then, we simulate the cascading failure process of power supply network, redistribute the electric power load in each of the remaining nodes, and finally remove the overload failed nodes (including their adjacent edges) and those nodes that are disconnected to source nodes. The cascading process will repeat until the power supply network achieves a new stable state again.

2.3. Assessment of Network Vulnerability. Based on the "dose-response" curve of network performance, we defined a new metric that can calculate the vulnerability of power supply network. The metric is shown as follows:

$$V = \frac{(A_N - A_P)}{A_N} = \frac{\left(\int_0^1 P_N d_h - \int_0^1 P(h)\, d_h\right)}{\int_0^1 P_N d_h} \tag{4}$$

where h represents the percentage of failed nodes, $h \in [0, 1]$. $P(h)$ refers to the network performance under a certain percentage h of failed nodes. P_N is a constant that refers to the initial performance of power supply network. Therefore, A_P

refers to the area under the $P(h)$ curve from h=0 to h=1 (e.g., in Figure 1, this is the grey area under Curve B or Curve C). A_N refers to the rectangle area under the initial performance P_N from h=0 to h=1.

From formula (4), we can see that the vulnerability of network increases with the decline of area A_P. In practice, P_N equals 1, and $P(h)$ can be expressed as the ratio of actual network performance under h percentage of failed nodes to actual performance of original network. Therefore, after normalization, the vulnerability V of power supply network can be formulated as

$$V = 1 - \frac{A_P}{A_N} = 1 - \frac{\int_0^1 P(h)\, d_h}{\int_0^1 P_N d_h} \tag{5}$$

3. Case Study

To demonstrate the application of "dose-response" vulnerability assessment framework, we used an urban power supply network in east China as a case study. In this study, we thoroughly investigated how the structural and functional performance varied under different event scenarios (i.e., different event scale and types). Then we analyzed the "dose-response" curve of network performance in both two dimensions, calculated the vulnerability of network, and proposed several practical suggestions for supporting the decision-making processes that underpin the resilience and sustainability of urban power supply network.

3.1. Graph Representation and Background Information. Structurally, urban power supply network generally consists of power plant (source node), power substation (transmit node or source node), power transmission line, and power consumer. The urban power supply network in the case study is located in the northeast of Jiangsu province, on the Haizhou Gulf, which has two power plants and 72 substations at all levels from 550kv to 35kv. In these substations, 68 substations nodes are pure transmit nodes, and 4 substations nodes are also responsible for accepting electric power from outside. Therefore, there are 6 source nodes and 68 transmit nodes in the network.

Figure 4 shows the backbone graphical model of the urban power supply network in the case study. In the network, there are 6 source nodes (red color) and 68 transmit nodes (black color). The edges in the model generally refer to all types of transmission lines.

3.2. Different Event Scale and Types Input. As a foundation to unified approach of sustainability and resilience, the "dose-response" vulnerability assessment should cover a variety of events from small normal events to extreme events. However, it is difficult to find a unified standard to measure the scale of all events; thus we use the percentage of impacted nodes directly caused by the event to represent the event scale. In this framework, we consider two event types: random type and intentional type. In random type, the nodes directly impacted by the given event are randomly selected and removed. In intentional type, we recognize

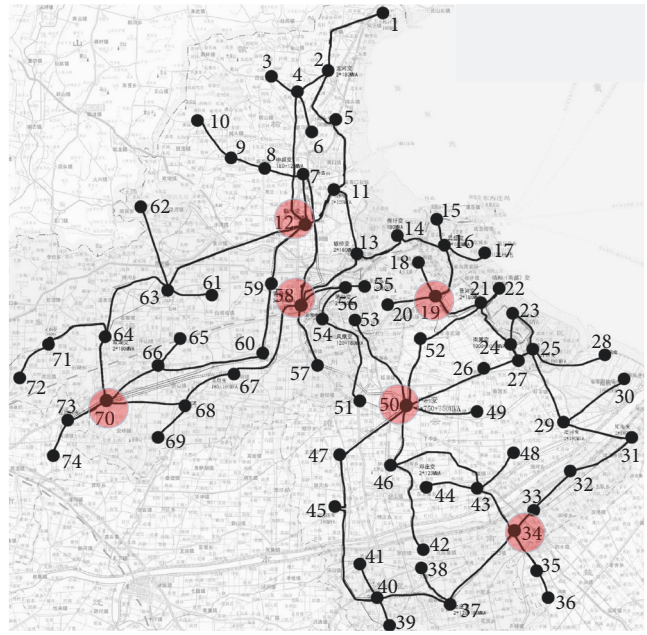

Figure 4: Graphical representation of the power supply network in the case study.

that the more important the nodes in the network, the more likely they are to be impacted [25, 26]. Therefore, in intentional type, the nodes directly impacted by the given event are selected according to their degree importance and betweenness importance, respectively.

3.3. Cascading Failure of Network. The cascading failure within the network will occur after the initial impact caused by the event. The given event will firstly impact a certain proportion of nodes in the network. After that, the power load of each residual node network will redistribute, and some of residual nodes will fail and be removed due to power overload. Then, a new round of load redistribution will occur until the final stable state of the network is achieved.

In the case study, to explore the internal cascading failure of urban power supply network, we choose the Motter model to simulate the cascading failure mechanism of urban power supply network [27, 28]. According to available studies, Motter model is a classical and widely used model to describe the cascading failure mechanism of critical infrastructure network, which can reasonably simulate the flow distribution of infrastructure network [29]. In Motter model, the possibility of describing cascading failures is enabled by assigning flow capacities to each of the nodes of the network. If any of these capacities is exceeded during power transmission, flow redistribution takes place to maintain the supply-demand balance of the network. For any node k in the network, the node betweenness P_k is used as an approximation of the load L_k that flows through each node k. Since engineered

infrastructure system is optimized for maximum capacity and minimum cost, the maximum allowable load C_k is proportional to the initial load L_k [27–30]:

$$C_k = (1 + \alpha) L_k \tag{6}$$

where initial load L_k of node k is expressed by the node betweenness P_k [27–30]. $\alpha \geq 0$ is the tolerance parameter or added flow capacity relative to the original capacity; thus we call α the redundancy coefficient of node. If the load of node k exceeds its maximum threshold C_k, the node quits operation. Despite the simplicity of the α concept, this parameter allows a systematic evaluation of the aggregated effects of network element overdesign on cascading failure containment.

3.4. Simulation Procedure for Assessing Network Performance. To generate the "dose-response" curve of network performance (with event scale and types), we completed a simulation procedure (Figure 5) to obtain the network performance under certain event scale and type according to the proposed framework (Figure 2). The following key aspects of this simulation should be noted.

First, for different event types, we use different methods to obtain the performance value under certain event scale. For random type, due to the randomness of nodes directly impacted by the event, a single simulation cannot determine the network performance under the event. Therefore, in random type, we take the average value of 500 times simulation results as the final network performance value under certain event. For intentional type, the nodes directly impacted by the event are chosen according to their importance. Thus, a single simulation run is enough to determine the network performance value after the occurrence of event.

Second, no matter whether in random type or intentional type, the cascading failure of power supply network is needed to be thoroughly simulated in the procedure. The cascading failure simulation is conducted according to the rule of Motter model introduced in Section 3.3.

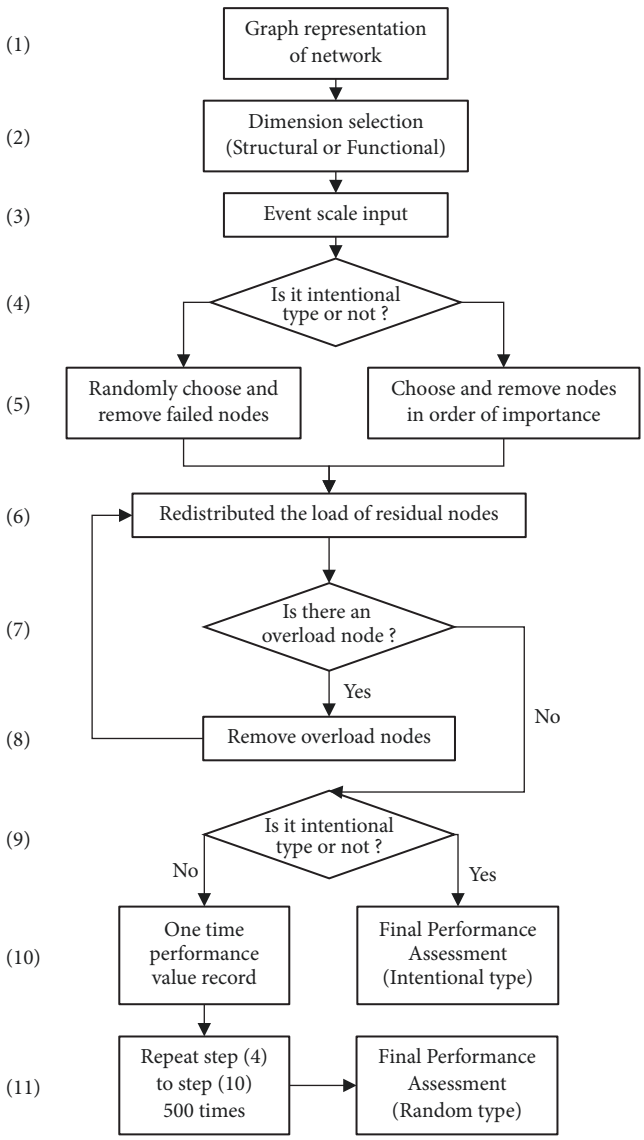

Figure 5: Simulation procedure for assessing the network performance under certain event.

4. Results and Discussion

4.1. Importance Ranking of Network Nodes. To assess the vulnerability of power supply network in the intentional type of event, we need to rank the importance of network nodes according to their degree and betweenness, respectively [21]. For the urban power supply network proposed in this case study, the results of the importance ranking based on node degree and node betweenness are shown in Figure 6.

4.2. "Dose-Response" Curve of Power Supply Network. For the urban power supply network proposed in this case study, the "dose-response" curves which express the variation of network performance with the scale of failed nodes in structural dimension and functional dimension are shown in Figures 7 and 8, respectively.

4.2.1. Structural Dimension. As shown in Figure 7, structural performance P_S of power supply network decreased with the increase of failed nodes, no matter whether under random events or intentional events. The structural vulnerability of network to intentional type of events was greater than that to random type of events.

Under intentional type of events, when the percentage of failed nodes reached 25%, the structural performance dropped to less than 0.2 and the network structure was almost paralyzed, regardless of whether it was based on the degree or betweenness.

Under random type of events, when percentage of failed nodes reached 25%, the structural performance approximately dropped to 0.5. Even when 60% of nodes randomly failed, the structural performance could remain more than 0.2. This is because intentional attack primarily chose the most important nodes in the network to impact, which often resulted in a quicker structure collapse of power supply network. Furthermore, the failure of most important nodes

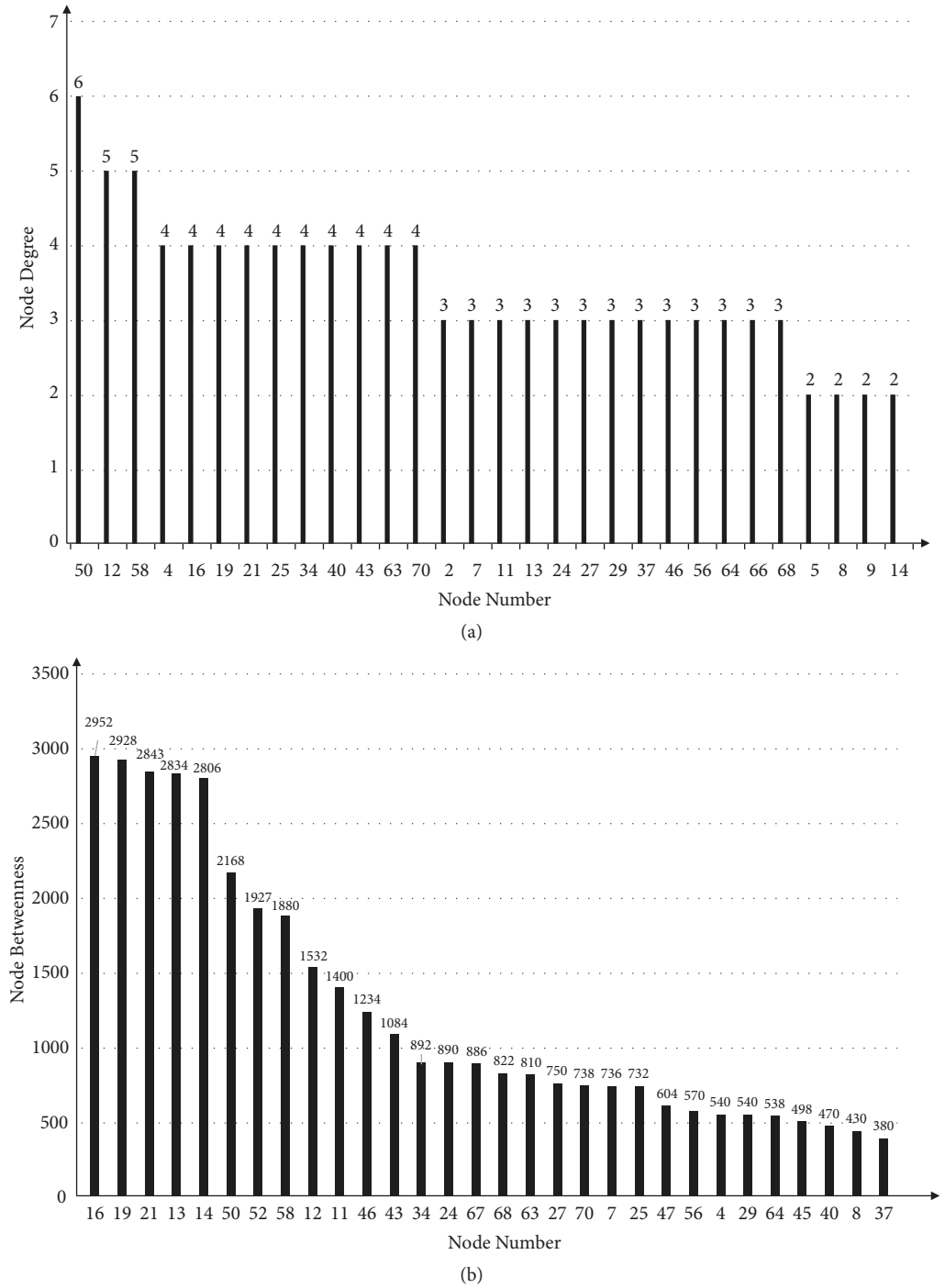

Figure 6: Importance ranking of network nodes: (a) according to node degree; (b) according to node betweenness.

will also exacerbate the cascading effect in the power supply network.

For two types of intentional events, the structural vulnerability to degree-based attack was obviously greater than that to betweenness-based attack, especially when the percentage of failed nodes was within 40%. The structural performance under degree-based attack was significantly lower than that under the betweenness-based attack. This phenomenon indicates that the intentional event based on node degree more obviously accelerated the disintegration of the power supply network structure, which led to a serious decline of structural performance. When the percentage of the failed nodes under intentional event was over 40%, the structural performance of power supply network under degree-based attack, which decreased to less than 0.1, was very close to that under betweenness-based attack. From this point, the

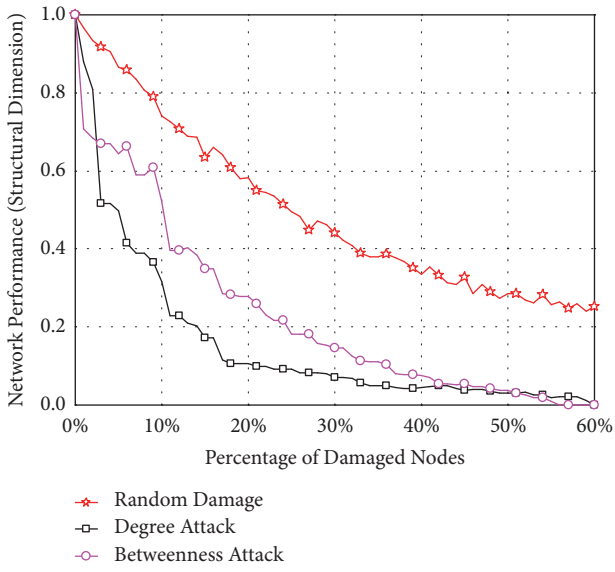

FIGURE 7: Variation of structural performance P_S with the percentage of failed nodes.

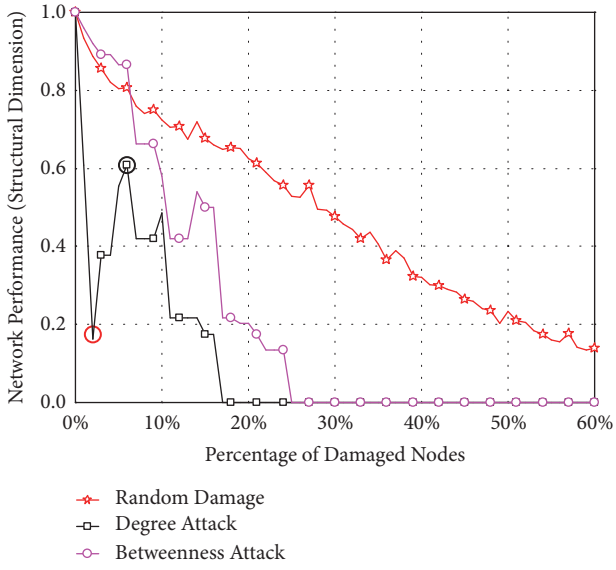

FIGURE 8: Variation of functional performance P_F with the percentage of failed nodes.

basic structure of power supply network almost completely collapsed.

4.2.2. Functional Dimension. It can be observed from Figure 8 that the "dose-response" curve of network in functional dimension is quite different from that in structural dimension shown in Figure 7.

For random type of events, the decrease of functional performance is relatively slow, which is similar to that in structural dimension. But for intentional type of events, the function of the power supply network decreased rapidly. When the percentage of failed nodes reached 25%, the function was completely lost. To the power supply network proposed in this case study, effective measures should be taken as early as possible to keep the percentage of failed nodes within 25% under intentional events; otherwise the structure and function of network will easily be completely paralyzed.

Focusing on the "dose-response" curve based on intentional event showed in Figure 8, functional performance first decreased quickly to a minimum point with the increase scale of failed nodes and then visibly rebounded to a maximum point. Finally, the functional performance continued to gradually decrease with the increasing scale of failed nodes. The rebound on the curve based on degree-based attack was more visible. This is because the degree-based attack on important nodes vastly exacerbated the cascading effect inside the power supply network. Firstly, degree-based attack impacted a few of nodes in the initial stage. Then, the load redistribution led to a cascading failure, which resulted in overload and failure of more nodes. After that, network function decreased rapidly to a minimum point.

In order to further illustrate the reason why functional performance has a visible rebound under degree-based attack, the betweenness of each node with the functional performance on maximum point and minimum point (i.e., black circle and red circle in Figure 8) is shown in Figure 9. When the functional performance of network reached the minimum point (red circle in Figure 8), large-scale nodes exceeded their own maximum threshold C_k (see the red bar in Figure 9) and then became overloaded and out of operation. With the increasing percentage of failed nodes directly caused by the event, the overall loading situation became better and the proportion of overloaded nodes became lower (see the black bar in Figure 9). Thus, the cascading failure effect was not obvious and the functional performance rebounded to maximum point (black circle in Figure 8). Subsequently, with further increase of failed nodes directly caused by the event, functional performance of power supply network continued to decrease rapidly due to the collapse of network structure.

4.3. Vulnerability Assessment of Power Supply Network. According to the "dose-response" curves proposed in Section 4.2, the vulnerability of power supply network in different dimensions can be calculated. As Figure 10 shows, no matter whether under random events or intentional events, the structural vulnerability is very close to the functional vulnerability. What is more, in both dimensions, the vulnerability of power supply network under intentional type of events is much higher than that under random type of events. For intentional type of events, the vulnerability of power supply network under degree-attack is a little higher than that under betweenness-attack.

4.4. Relationship between Redundancy Coefficient α and Network Vulnerability. In Section 3.3, redundancy coefficient α was introduced to represent the capacity of node to tolerate a load that exceeds the rated load. From the perspective of network system, the redundancy coefficient α actually reflects the safety factor that directly impacts the vulnerability of

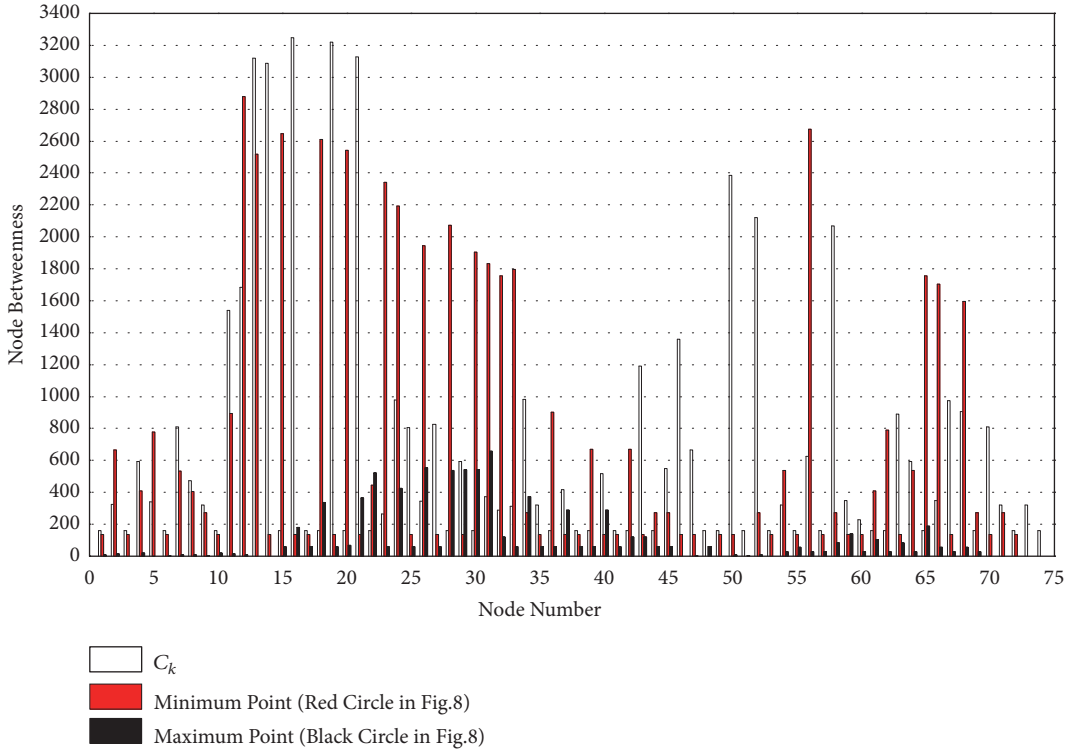

Figure 9: Load comparison of each node on different status of functional performance. (White bar: maximum load threshold C_k of each node. Red bar: load of each node when the functional performance reached minimum point in Figure 8. Black bar: load of each node when the functional performance reached maximum point in Figure 8.)

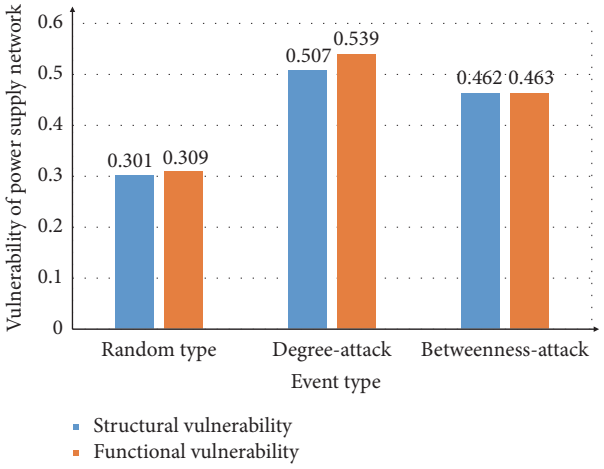

Figure 10: Vulnerability of power supply network in different dimensions.

the power supply network. However, excessive increase of redundancy coefficient α is an overreaction which is not conducive to the sustainable development of urban power supply network. Therefore, it is important to optimize the redundancy coefficient α of urban power supply network.

The "dose-response" vulnerability results of the power supply network presented in Section 4.2 were obtained under the assumption that redundancy coefficient α was equal to 0.1. In fact, the vulnerability of network under different types of events is closely related to redundancy coefficient α. Considering that structural performance is an inherent property of the network and redundancy coefficient α mainly affects the network function property, we discuss the relationship between the functional performance P_F of network and redundancy coefficient α under different types of events (see Figure 11). This provides a theoretical guidance for the optimal setting of redundancy coefficient for the urban power supply network.

It can be observed from Figure 11 that redundancy coefficient α had a direct influence on the functional performance of the power supply network. The functional performance increased with redundancy coefficient α when α is within a certain interval. Then, when α reached a certain threshold, network performance tended to be stable and no longer increased with it any more. Therefore, an appropriate redundancy coefficient α is beneficial for the economical efficiency and sustainable development of urban power supply network.

Figures 11(a), 11(b), and 11(c) have shown the variation of functional performance P_F with redundancy coefficient α and percentage of failed nodes under different types of events. From these figures, we can preliminarily figure out the minimum effective threshold of redundancy coefficient α that will obviously improve the functional performance under different scale and types of events (see Tables 1 and 2).

As shown in Table 1, if the decision-maker wants to improve the functional performance to more than 0.7 under

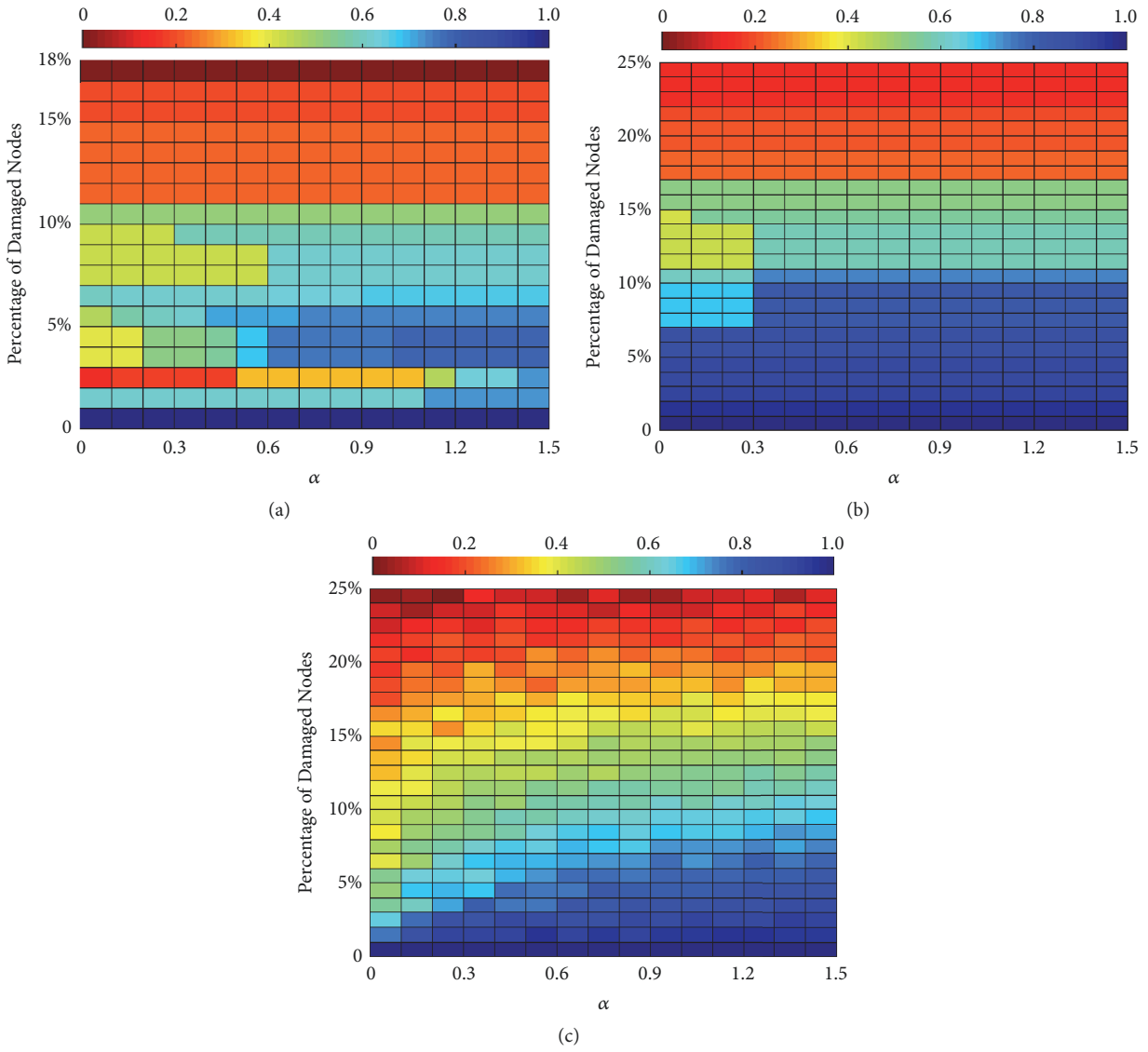

FIGURE 11: Variation of functional performance P_F with redundancy coefficient α and percentage of failed nodes: (a) degree-based attack, (b) betweenness-based attack, and (c) random events.

a certain scale of failed nodes, the most economical value of redundancy coefficient α can be figured out in detail. It has to be noted that when the scale of failed nodes is too large, there will be no redundancy coefficient α that can meet the requirement. If the decision-maker wants to improve the functional performance to another value such as 0.5, the most economical value of redundancy coefficient α can also be figured out in detail from Figure 11 (see Table 2).

5. Conclusions and Future Study

As a foundation of unified study of sustainability and resilience for urban power supply network, the "dose-response" vulnerability assessment framework that focuses on both structural and functional dimensions for urban power supply network was proposed in this paper. The proposed framework is also suitable for both two types of events (i.e., random type and intentional type). To illustrate the framework, the power supply network of a city in east China was taken as an example to conduct vulnerability assessment. Through this case study, "dose-response" interrelationships between the structural performance, functional performance, and event scale in both random and intentional type of events were thoroughly discussed and analyzed. Then the network vulnerability under different types of events was calculated, and the redundancy coefficient α of urban power supply network was optimized. These interrelationships and conclusions can be foundational information for the further unified approach of sustainability and resilience.

Based on the "dose-response" vulnerability framework for power supply network proposed in this work, there are some extending studies that can be conducted in the future.

First, "dose-response" vulnerability assessment was primarily conducted in the structural dimension and functional

Table 1: Minimum effective threshold of α on the functional performance ($P_F \geqslant 0.7$).

Event type		Scale of failed nodes				
		5%	10%	15%	20%	25%
Intentional	Degree-based	α=0.5	—	—	—	—
	Betweenness-based	α=0	α=0.3	—	—	—
Random		α=0.1	—	—	—	—

Note: (1) Table 1 focuses on the minimum threshold of α that can improve the functional performance to more than 0.7 (i.e., $P_F \geqslant 0.7$); (2) "—" means no α can meet the requirement.

Table 2: Minimum effective threshold of α on the functional performance ($P_F \geqslant 0.5$).

Event type		Scale of failed nodes				
		5%	10%	15%	20%	25%
Intentional	Degree-based	α=0.2	α=0.3	—	—	—
	Betweenness-based	α=0	α=0	—	—	—
Random		α=0	α=0.1	—	—	—

Note: (1) Table 2 focuses on the minimum threshold of α that can improve the functional performance to more than 0.5 (i.e., $P_F \geqslant 0.5$); (2) "—" means no α can meet the requirement.

dimension as a foundation research for the unified study of sustainability and resilience of power supply network. For the infrastructure system such as power supply network, the event will firstly impact the structural dimension and functional dimension, and then the impact will spread to social, economic, and ecological dimension. Therefore, it is important to apply this framework to other extended dimensions such as social dimension, economic dimension, and ecological dimension.

Second, the vulnerability research of critical infrastructure network is gradually expanding from a single infrastructure network infrastructure to interdependent infrastructure networks [31–33]. The urban power supply network is at the very heart of modern critical infrastructure systems. The failure of power supply network will inevitably lead to a severe disturbance of other infrastructure networks. Thus, for the resilient and sustainable development of the whole city, it is necessary to expand the "dose-response" vulnerability assessment framework to urban interdependent infrastructure networks including power supply network.

Data Availability

Our original data form is at https://pan.baidu.com/s/1mFy7X9bKZebh5OljGBS5uA. Password: 3u53. The "Research data" includes six sheets. "Node degree" and "node betweenness" were the initial state of the network, which was used to determine the attack sequence. "Structural dimension performance" includes the EL in three attack modes. The rest of 3 sheets reflect the relationship between redundancy coefficient α and network performance CL. Finally, the folder includes all betweenness of each node in different disaster and different intensity.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors appreciate the data and information supports from the City Construction Bureau and Municipal Design and Research Institute of Lianyungang City, China. The authors thank Doctor Huang for her valuable comments and suggestions. This work was supported by National Natural Science Foundation of China (51708554).

References

[1] E. A. Piana, F. Bignucolo, A. Donini, and R. Spezie, "Maintenance of a high-voltage overhead transmission line: Sustainability and noise impact assessment," *Sustainability*, vol. 10, no. 2, 2018.

[2] X. Xu, D. Niu, J. Qiu, P. Wang, and Y. Chen, "Analysis and optimization of power supply structure based on Markov chain and error optimization for renewable energy from the perspective of sustainability," *Sustainability*, vol. 8, no. 7, 2016.

[3] M. Panteli and P. Mancarella, "Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies," *Electric Power Systems Research*, vol. 127, pp. 259–270, 2015.

[4] P. Bocchini, D. M. Frangopol, T. Ummenhofer, and T. Zinke, "Resilience and sustainability of civil infrastructure: Toward a unified approach," *Journal of Infrastructure Systems*, vol. 20, no. 2, Article ID 04014004, 2014.

[5] Y. Y. Haimes, "On the definition of resilience in systems," *Risk Analysis*, vol. 29, no. 4, pp. 498–501, 2009.

[6] X. Zhao, H. Cai, Z. Chen, H. Gong, and Q. Feng, "Assessing urban lifeline systems immediately after seismic disaster based on emergency resilience," *Structure and Infrastructure Engineering*, vol. 12, no. 12, pp. 1634–1649, 2016.

[7] M. Ouyang, L. Dueñas-Osorio, and X. Min, "A three-stage resilience analysis framework for urban infrastructure systems," *Structural Safety*, vol. 36-37, pp. 23–31, 2012.

[8] Y. Y. Haimes, "On the definition of vulnerabilities in measuring risks to infrastructures," *Risk Analysis*, vol. 26, no. 2, pp. 293–296, 2006.

[9] E. Jenelius, T. Petersen, and L.-G. Mattsson, "Importance and exposure in road network vulnerability analysis," *Transportation Research Part A: Policy and Practice*, vol. 40, no. 7, pp. 537–560, 2006.

[10] A. Yazdani, R. A. Otoo, and P. Jeffrey, "Resilience enhancing expansion strategies for water distribution systems: a network theory approach," *Environmental Modelling & Software*, vol. 26, no. 12, pp. 1574–1582, 2011.

[11] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research*, vol. 81, no. 7, pp. 1334–1340, 2011.

[12] M. Rosas-Casals, S. Valverde, and R. V. Solé, "Topological vulnerability of the European power grid under errors and attacks," *International Journal of Bifurcation and Chaos*, vol. 17, no. 7, pp. 2465–2475, 2007.

[13] Å. J. Holmgren, "Using graph models to analyze the vulnerability of electric power networks," *Risk Analysis*, vol. 26, no. 4, pp. 955–969, 2006.

[14] V. Latora and M. Marchiori, "Vulnerability and protection of infrastructure networks," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 71, no. 1, Article ID 015103, 2005.

[15] T. C. Matisziw, A. T. Murray, and T. H. Grubesic, "Exploring the vulnerability of network infrastructure to disruption," *Annals of Regional Science*, vol. 43, no. 2, pp. 307–321, 2009.

[16] M. Bruneau, S. E. Chang, R. T. Eguchi et al., "A framework to quantitatively assess and enhance the seismic resilience of communities," *Earthquake Spectra*, vol. 19, no. 4, pp. 733–752, 2003.

[17] S. E. Chang and M. Shinozuka, "Measuring improvements in the disaster resilience of communities," *Earthquake Spectra*, vol. 20, no. 3, pp. 739–755, 2004.

[18] Xu. Zhao, Z. Chen, and H. Gong, "Effects Comparison of Different Resilience Enhancing Strategies for Municipal Water Distribution Network: A Multidimensional Approach," *Mathematical Problems in Engineering*, vol. 2015, Article ID 438063, 16 pages, 2015.

[19] K. A. Anarde, S. Kameshwar, J. N. Irza et al., "Impacts of Hurricane Storm Surge on Infrastructure Vulnerability for an Evolving Coastal Landscape," *Natural Hazards Review*, vol. 19, no. 1, 2018.

[20] M. Ouyang, "Comparisons of purely topological model, betweenness based model and direct current power flow model to analyze power grid vulnerability," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 23, no. 2, 2013.

[21] V. Latora and M. Marchiori, "How the science of complex networks can help developing strategies against terrorism," *Chaos, Solitons & Fractals*, vol. 20, no. 1, pp. 69–75, 2004.

[22] A. Nagurney and Q. Qiang, "A network efficiency measure with application to critical infrastructure networks," *Journal of Global Optimization*, vol. 40, no. 1–3, pp. 261–275, 2008.

[23] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the North American power grid," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 69, no. 2, Article ID 025103, 2004.

[24] K. Poljanek, F. Bono, and E. Gutiérrez, "Seismic risk assessment of interdependent critical infrastructure systems: The case of European gas and electricity networks," *Earthquake Engineering & Structural Dynamics Journal*, vol. 41, no. 1, pp. 61–79, 2015.

[25] S. Sayyadipour, G. R. Yousefi, and M. A. Latify, "Mid-term vulnerability analysis of power systems under intentional attacks," *IET Generation, Transmission & Distribution*, vol. 10, no. 15, pp. 3745–3755, 2016.

[26] H. S. Jeong, J. Qiao, D. M. Abraham, M. Lawley, J.-P. Richard, and Y. Yih, "Minimizing the consequences of intentional attack on water infrastructure," *Computer-Aided Civil and Infrastructure Engineering*, vol. 21, no. 2, pp. 79–92, 2006.

[27] A. E. Motter, "Cascade control and defense in complex networks," *Physical Review Letters*, vol. 93, no. 9, Article ID ID098701, 4 pages, 2004.

[28] A. E. Motter and Y. Lai, "Cascade-based attacks on complex networks," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 66, no. 6, Article ID 065102, 4 pages, 2002.

[29] L. Dueñas-Osorio and S. M. Vemuru, "Cascading failures in complex infrastructure systems," *Structural Safety*, vol. 31, no. 2, pp. 157–167, 2009.

[30] L. Zhao, K. Park, and Y.-C. Lai, "Attack vulnerability of scale-free networks due to cascading breakdown," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 70, no. 3, Article ID 035101, 2004.

[31] M. Ouyang, "Review on modeling and simulation of interdependent critical infrastructure systems," *Reliability Engineering & System Safety*, vol. 121, pp. 43–60, 2014.

[32] T. L. Ng and X. Cai, "Relationships between Interdependency, Reliability, and Vulnerability of Infrastructure Systems: Case Study of Biofuel Infrastructure Development," *Journal of Infrastructure Systems*, vol. 20, no. 1, p. 04013008, 2014.

[33] L. Dueñas-Osorio, J. I. Craig, B. J. Goodno, and A. Bostrom, "Interdependent response of networked systems," *Journal of Infrastructure Systems*, vol. 13, no. 3, pp. 185–194, 2007.